

SECURITY SERVICES AGREEMENT

Between the

National Business Center (NBC)

and

Indian Health Service (IHS)

August 2005

Page 1 of 10

This Document Contains Sensitive But Unclassified Information
Do not remove this notice
Properly destroy when no longer needed

**INFORMATION TECHNOLOGY (IT)
SECURITY SERVICES AGREEMENT**

BETWEEN THE NBC

AND

IHS

I. AUTHORITY.

This Security Services Agreement (SSA) satisfies the requirements of the Office of Management and Budget (OMB) Circular A-130, Appendix III, and is made and entered into between the NBC and IHS, referred to CUSTOMER throughout the rest of this document, as acknowledged by the signatures of the appropriate representatives on the signature section of this document.

II. BACKGROUND.

It is the intent of the National Business Center (NBC) to provide its clients with high quality, responsive and responsible computer and information security services commensurate with the sensitivity and criticality of client data and applications. NBC IT Security consists of a staff of highly trained professionals whose sole function is serving the IT Security needs of the NBC and its clients. The NBC operates under the premise that IT Security services involve dual responsibilities that are shared between the NBC and its client organizations. This premise is reflected throughout this document and in every service provided to NBC client organizations.

III. PURPOSE.

The purpose of this SSA is to clearly establish and document NBC and client security roles and responsibilities.

IV. RESPONSIBILITIES.

This SSA covers IT Security for the QMIS system.

**SECTION A: NBC RESPONSIBILITIES AND NBC EXPECTATIONS
RELATING TO CLIENT ORGANIZATIONS**

1. The NBC:

- Publishes policies, standards, and procedures relating to all aspects of computer and information security.
- Conducts continuity of operations planning to ensure the recoverability and continuity of QMIS Program Management services for all QMIS clients in the event of a disaster or other unplanned outage.
- Maintains current certification and accreditation (C&A) documentation for QMIS. Proof of authority to operate (ATO) documents will be provided to clients on request.
- Conducts regular security assessments and tests as prescribed in the Federal Information Security Management Act (FISMA) of 2002 and the National Institute of Standards and Technology (NIST) Special Publication 800-26, "Security Self-Assessment Guide for Information Technology Systems."
- Ensures that appropriate background investigations are conducted for NBC employees and contractors.
- Ensures that all NBC employees and contractors receive initial security awareness training before being given access to NBC-managed computer systems, and annual follow-up security awareness training as required by OMB Circular A-130, Appendix III, Department of the Interior Departmental Manual 375, Chapter 19, and the NBC Computer and Information Security Policy (NBC-CIO-POL-001).
- Endeavors to ensure through the use of policies and awareness training, that all NBC employees and contractors know how to identify sensitive or restricted information, and that they comply with requirements for marking, handling, disclosing, releasing, storing, retaining, copying or backing up, disposing of, sanitizing, or destroying such information.
- Provides clients with reasonable assurance that IT resources (data files, application programs, and computer-related facilities and equipment) are protected against unauthorized modification, disclosure, loss, or impairment. Such controls include physical controls, (e.g., keeping computers in locked rooms to limit physical access), logical controls (e.g.,

August 2005

security software programs designed to prevent or detect unauthorized access to sensitive files), and personnel controls (e.g., background checks, security clearances, etc.).

- Follows stringent requirements of the Department of the Interior, and bureau-wide policies and guidelines requiring the use of firewalls, intrusion detection systems (IDS), and computer security incident response capabilities.
- Applies appropriate communications security, in accordance with OMB and Departmental policies and standards.
- Uses antivirus software and ensures that current versions are used on all equipment, to include procedures for ensuring that portable devices such as laptops are updated as often as possible.
- Enforces the use of individually assigned User IDs and secret passwords that must be changed on a standardized cycle of password aging.
- Employs security procedures that apply when employees terminate employment or change jobs.
- Routinely monitors activity against sensitive application and system files to detect indicators of misuse or abuse and notifies clients whenever evidence of misuse or abuse of client data has been detected.
- Acts as Subject Matter Experts (SME) for computer and information security matters for the NBC and on behalf of NBC clients.
- Provides a Computer Security Incident Response Capability in the event of a successful penetration attack against an NBC system and notifies clients whenever a computer security incident occurs that involves or threatens the client's application or data.

2. The CUSTOMER agrees to be responsible for:

- Providing security for the QMIS system at each end-user location. Individuals assigned this responsibility would be expected to interact with the NBC QMIS Program Manager, or with the NBC IT Security staff in resolving problems or issues relating to the security and protection of the QMIS system.
- Establishes and maintains policies and procedures for performing regular data backups, and for storing backups securely, in the event of a disaster or other outage that would require recovery of the system.
- Administering security on the QMIS computer system in accordance with all requirements of the NBC Rules of Behavior attached to this SSA.

- Acknowledging that the security of CUSTOMER data is ultimately the responsibility of the CUSTOMER organization. Except for the actions of CUSTOMER end-users, the NBC is responsible for the security of CUSTOMER data if it is housed in the NBC data center.
- Reporting to NBC IT Security any security events or incidents at a CUSTOMER site that might threaten or negatively impact the integrity or availability of the NBC network or of any NBC-managed computer system.
- Cooperating with the NBC Computer Security Incident Response Team (CSIRT) in the event of a successful security penetration or other breach so that evidence may be collected and preserved and the security of the network or system can be restored.

3. The CUSTOMER individual(s) responsible for the security of the QMIS system, for client organizations whose employees and contractors have a business need to access the QMIS system is(are) responsible to:

- Ensure that the employees and contractors of the CUSTOMER organization behave in a manner that is appropriate to the use and protection of the QMIS system, based on applicable government security guidelines and recommendations.
 - An application-specific rules of behavior (ROB) for NBC-managed systems is attached to this Security Services Agreement (SSA). This ROB document is provided in compliance with OMB Circular A-130, Exhibit III, paragraph 3., a., 2), a). The ROB should be removed from the SSA by the customer. The ROB may be used at the CUSTOMER'S discretion to ensure that QMIS users behave in a manner appropriate for the security and protection of the QMIS computer system.
- Authorize the NBC QMIS Program Manager, by signing this SSA, to access CUSTOMER QMIS data submitted to the QMIS Program Manager, to the extent necessary to perform normal QMIS operational functions (e.g., for data backup and recovery, reporting purposes, or any other appropriate business needs), as may be required.

4. Whenever CUSTOMER employees and contractors have a business need to access the QMIS computer system, CUSTOMER agrees to be responsible for implementing and overseeing user compliance with appropriate security-related activities. For example, the CUSTOMER agrees to endeavor to ensure that QMIS users:

- Use the QMIS computer system and associated data for work-related

August 2005

purposes only.

- Lock the workstation keyboard or log off when leaving the workstation area to prevent unauthorized use of the workstation.
- Are responsible for the appropriate use and protection of sensitive information to which he/she has authorized access.
- Immediately report all computer security incidents (viruses, intrusion attempts, system compromises, etc.) to the CUSTOMER individual who is assigned security responsibility for the QMIS computer system.

SECTION B: CLIENT-SPECIFIC REQUIREMENTS AND EXPECTATIONS RELATING TO THE NBC

Client specific security service requirements that are not addressed in the main SSA are documented in this Section. At a minimum, this section should include the following information:

INFORMATION SENSITIVITY: Indicate your responses to the following:

- a. **CUSTOMER QMIS information may contain (Check all that apply):**

☐ Privacy Act ☐ Sensitive But Unclassified (SBU)

☒ Non-sensitive (same as 'public') ☐ Other

If "Other" please describe: _____

- b. Please note any additional security-related services the CUSTOMER requires or expects to receive from the NBC, that are not already covered in the SSA.

August 2005

V. NBC IT SECURITY CONTACTS.

A. NBC

NAME	TITLE	PHONE #	FAX #	E-MAIL
Bob D. Haycock	OS/NBC CIO	(303) 969-7188	(303) 969-7102	Bob_D_Haycock@nbc.gov
Mary H. Macleod	NBC IT Security Manager	(303) 969-7126	(303) 969-7102	Mary_H_Macleod@nbc.gov
Jeanne M. Tallent	Alternate NBC IT Security Manager	(703) 390-6726	(703) 390-6780	Jeanne_M_Tallent@nbc.gov
QMIS Help Desk	Quarters Program Manager	(303) 969-5050	(303) 969-6634	Doug_B_Pokorney@nbc.gov

Information Technology Security Services Agreement (SSA)

PARTIES TO THE AGREEMENT:

Signed on behalf of
the NBC:


Bob D. Haycock
Chief Information Officer
Office of the Secretary/National Business Center

Date: _____

Mary H. Macleod
OS/NBC IT Security Manager
Office of the Secretary/National Business Center

Date: _____

Signed on behalf of
the CUSTOMER:


James R. Biasco, P.E.
Director
Division of Facilities Operations
Office Of Environmental Health and Engineering
Indian Health Service

Date: 10/11/05

Signature

Date: _____

Title

Name of Client Organization

Period of Agreement: In consideration of the termination provisions stated in the Inter/Intra Agency Agreement, this Security Services Agreement may be terminated by written notice from either party, or by written mutual agreement between the parties.

August 2005

RULES OF BEHAVIOR FOR CLIENT USERS OF THE QMIS COMPUTER SYSTEM MANAGED BY THE DEPARTMENT OF THE INTERIOR, NATIONAL BUSINESS CENTER

The following Rules of Behavior (ROB) apply to all client users of the QMIS computer system managed by the Department of the Interior (DOI), National Business Center (NBC). These ROB should be made available to all users before granting them access to QMIS. They are intended to supplement any existing organizational ROB that might be in use by client organizations.

1. Applicability and Supporting Documentation

For client users employed by a bureau of the DOI, this ROB complies with OMB Circular A-130, Appendix III, and supplements DOI Departmental Manual 375, Chapter 19.

For non-DOI client users subject to OMB requirements, this ROB complies with OMB Circular A-130, Appendix III, and is intended to supplement the client organization's information security policies, standards and ROB.

For non-DOI clients NOT subject to OMB directives, this ROB should be considered as recommended behavior for client users, to assist the NBC in maintaining the highest possible security protections for client data, and for the QMIS computer system.

2. Universal Client User ROB

2.2 General Client User Responsibilities

- Client users are responsible for using NBC-managed computer systems and associated data for business purposes only.
- Client users of NBC-managed systems and applications may not access, or attempt to access, data for which they are not authorized.
- Client users are responsible for protecting the confidentiality of data associated with the QMIS system, based on the sensitivity of the data. Such data may not be given to unauthorized persons.
- Client users should report suspected or actual security violations to their supervisor, the individual who is assigned security responsibility for QMIS or the QMIS Program Manager.

3. Consequences for Non-Compliance with these ROB

August 2005

**RULES OF BEHAVIOR FOR CLIENT USERS OF
THE QMIS COMPUTER SYSTEM MANAGED BY
THE DEPARTMENT OF THE INTERIOR,
NATIONAL BUSINESS CENTER**

The consequences of Federal employee or contractor behavior not consistent with these rules may result in revocation of access to the QMIS system by the QMIS security representative, and wherever such actions may be applicable, disciplinary action consistent with the nature and scope of the infraction may be applied according to the client organization's guidelines regarding disciplinary actions.